

Asia Internet Coalition (AIC) Industry Submission on Pakistan Draft Data Protection Bill 2023
(Private Member Bill), Proposed Redline Changes

8 May 2023

Honourable Mr. Syed Amin Ul Haque
Federal Minister for Information Technology and Telecommunication
Ministry of Information Technology and Telecommunication (MoITT)
7th Floor, Kohsar Block, Pak Secretariat,
Islamabad, Pakistan

Cc:

- *Chairperson Kauda Babar, Pakistan Senate Standing Committee (SSC)*
- *Honourable Prime Minister Muhammad Shehbaz Sharif, Prime Minister's Office, Islamabad, Pakistan*

On behalf of the [Asia Internet Coalition](#) (AIC) and its members, we would like to thank the Government of Pakistan and the Ministry of Information Technology and Telecommunication (“**MOITT**”) for the opportunity to respectfully submit further comments on the Data Protection Bill 2023, which was moved by Senator Afnan Ullah Khan as a Private Member Bill before the Pakistani Senate on 13 February 2023 (the “**Bill**”). This submission (**In Redline Changes**) is a follow-up to the letter dated 3 April 2023 and submitted to the Pakistan Senate Standing Committee (SSC).

While both previous and latest MOITT Draft Bills provide certain additional legal basis for the cross-border transfer of personal data, we find that the Draft Bill still does not address the majority of industry’s substantive concerns of stringent limitations on cross-border data flows and mandatory data localization. The Private Member’s Bill only enables cross-border transfer if it is determined that the jurisdiction to which data is being exported offers equivalent protection. These provisions fall short of international standards for data protection (such as GDPR) and will adversely impact Pakistani consumers and businesses. In its current form, we believe that the Bill will have a negative impact on the ability of foreign internet companies to trade with and operate in Pakistan, hindering the country’s economic recovery and deterring foreign investment.

The protection of personal data is an important component of any privacy framework, and we appreciate the opportunity to provide feedback on the Draft Bill. AIC and its members have worked closely with governments around the world in relation to the development of national personal data protection policies and legislation. In doing so, we have witnessed first-hand the potential for such policies and legislation to effectively protect the privacy interests of citizens

without hindering innovation and technological advancement. We recognize the on-going efforts of the Government of Pakistan and MOITT in further fine-tuning the draft legislation, but we continue to have concerns, particularly on cross-border transfer of “critical” and “sensitive” personal data.

On this note, we express our continued interest to participate in opportunities for consultation to further assist the Government’s review of the Personal Data Protection Bill 2023.

Importantly, we trust that these comments and recommendations (In Appendix A with Redline changes) are useful and look forward to continuing our work with the Government of Pakistan, other industry players, consumer groups and all other relevant stakeholders to help deliver an effective and robust privacy framework for Pakistan based on international good practices.

The AIC also wishes to request for an industry meeting to better understand the views and priorities stemming from the Bill. This meeting can also discuss potential areas of collaboration as well as opportunities for consultation that can further assist the Government’s review of the Personal Data Protection Bill 2023. As such, we welcome a video conference meeting with you or your team at a date and time of your convenience.

Should you have any questions or need clarification, please do not hesitate to contact me directly at Secretariat@aicasia.org or +65 8739 1490. Thank you again for your time and consideration.

Thank you for your time and consideration.

Sincerely,



Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

Appendix A

Asia Internet Coalition (AIC) Industry Submission on Pakistan Draft Data Protection Bill 2023 (Private Member Bill), **Redline Changes**

Issue	Current Clause	Recommendation	Rationale
Effective date	1. SHORT TITLE, EXTENT, AND COMMENCEMENT. — (1) This Act may be called the Personal Data Protection Act, 2023. (2) It shall extend to the whole of Pakistan. (3) It shall come into force on such date as the Federal Government may, by notification in the Official Gazette for the commencement of this Act .	1. SHORT TITLE, EXTENT, AND COMMENCEMENT. — (1) This Act may be called the Personal Data Protection Act, 2023. (2) It shall extend to the whole of Pakistan. (3) It shall come into force on such date as the Federal Government may determine, by notification in the Official Gazette for the commencement of this Act by providing at least twenty-four months' advance notice from the effective date.	- It is critical that industry has sufficient time to prepare for compliance with the Act. - International experience demonstrates that several years is required to establish a regulator and build capacity in a country prior to enforcement of a privacy law. For example, the recently passed Indonesian privacy law provides for a 24 months grace period.
Data localisation and cross-border data flows	3. DEFINITIONS.— f) “Critical personal data” means data relating to public service providers, unregulated e-commerce transactions and any data related to international obligations; 30. RESTRICTIONS ON TRANSFERRING PERSONAL DATA.— 1. Every data fiduciary shall ensure personal data is stored on a server or data centre based in Pakistan. 2. The Commission shall notify such categories of personal data as critical personal data, from time to time, which shall not be transferred to any other territory outside	3. DEFINITIONS.— ~~f) “Critical personal data” means data relating to public service providers, unregulated e-commerce transactions and any data related to international obligations;~~ ~~30. RESTRICTIONS ON TRANSFERRING PERSONAL DATA.—~~ ~~1.—Every data fiduciary shall ensure personal data is stored on a server or data centre based in Pakistan.~~ ~~2.—The Commission shall notify such categories of personal data as critical personal data, from time to time, which shall not be transferred to~~	- The current draft of the Bill would require: - all personal data to be stored in Pakistan; and - very broad categories of “critical personal data” and “sensitive personal data” not to be transferred or processed outside Pakistan. - These requirements would be out of step with global privacy laws. No other APAC privacy laws include equivalent data localisation requirements. They would make the Pakistan privacy law the most restrictive privacy law that we are aware of. - Other countries that have contemplated adopting data localisation requirements have moved away from these proposals in recognition of the economic harm they would

Issue	Current Clause	Recommendation	Rationale
	Pakistan if not authorized by the Government. 3. Notwithstanding, anything contained in subsection (1), the Commission may notify certain categories of personal data as exempt from the requirement under subsection (1) on the grounds of public interest necessity, or strategic interests of Pakistan. 31. CONDITION FOR CROSS-BORDER TRANSFER OF PERSONAL DATA. — 1. Where personal data is required to be transferred beyond the borders of Pakistan to an entity/entities or system that is not under the direct control of the Government of Pakistan, the data fiduciary or a processor shall ensure that the country where the data is being transferred offers at least equivalent level of protection of personal data provided under this Act. 2. Any personal data other than those categorised as sensitive personal data may be transferred outside the territory of Pakistan under the conditions to be devised by the Commission. 3. The Commission shall also devise a mechanism for keeping some components of the sensitive personal data in Pakistan to which this Act applies, on the grounds of public interest of national security.	~~any other territory outside Pakistan if not authorized by the Government.~~ ~~3. Notwithstanding, anything contained in subsection (1), the Commission may notify certain categories of personal data as exempt from the requirement under subsection (1) on the grounds of public interest necessity, or strategic interests of Pakistan.~~ 31. CONDITION FOR CROSS-BORDER TRANSFER OF PERSONAL DATA. — 1. Where personal data is required to be transferred beyond the borders of Pakistan to an entity/entities or system that is not under the direct control of the Government of Pakistan, the data fiduciary or a processor shall ensure that the country where the data is being transferred offers at least equivalent level of protection of personal data provided under this Act. (2) The data fiduciary or processor shall be deemed to have fulfilled its obligation under sub-section (1) to ensure that the country to which the personal data is being transferred offers a level of protection which is at least equivalent to the protection provided under this Act if: a) the data fiduciary or processor enters into a legally binding and enforceable instrument with the recipient located outside Pakistan which obligates the recipient to protect the personal data so transferred to a standard at least equivalent to the protection under this Act; b) the transfer is made to a recipient located outside Pakistan which controls, is controlled by or is under common control with the data	produce, including India, Sri Lanka, Indonesia and Vietnam. - These requirements would put data at greater risk of a security breach and increase costs for businesses. They would significantly disincentivize foreign investment. Therefore, we recommend deleting the localisation requirements and introducing additional bases for transferring data out of Pakistan. - More specifically, the following changes should be made: - The category of “critical personal data” should be removed by deleting the definition in section 3(f) and the associated requirement to only store it in Pakistan in section 30(2). The definition of “critical personal data” is overly vague and there is therefore little certainty on what “critical personal data” will include. - The hard localisation requirement for “sensitive personal data” in section 31(2) should similarly be removed. - There is a soft localisation requirement to store all other personal data on a server or data centre in Pakistan by default under Section 30(1), although it does seem that such data can be transferred overseas where the conditions in section 30(1) are met. Mirroring of data also increases costs for businesses and security risks, we would recommend deleting this requirement. - We recommend several amendments to section 31(2) and (3) to introduce a number of lawful bases of overseas transfers which are consistent with several other international benchmarks.

Issue	Current Clause	Recommendation	Rationale
		fiduciary or processor, and pursuant to a set of binding corporate rules applicable to both the data fiduciary or processor and such recipient which obligates the recipient to protect the personal data so transferred to a standard at least equivalent to the protection under this Act; c) the transfer is pursuant to a code of conduct approved by the Commission with binding and enforceable commitments of the recipient outside of Pakistan to apply appropriate safeguards, including as regards to data principal's rights; or d) the transfer is pursuant to any other instrument, treaty or international certification recognized by the Commission which permits the transfer of personal data from Pakistan to the country in which the recipient is located. (3) Subsection (1) shall not apply to the extent that: a) The data principal has consented to the transfer of her personal data; b) The transfer is necessary for the performance of a contract between the data principal and the data fiduciary or processor, or the implementation of any pre-contractual measures taken by the data fiduciary or processor at the request of the data fiduciary; c) The transfer is reasonably necessary for the establishment, exercise or defence of actual or reasonably anticipated legal claims; d) The transfer is reasonably necessary for the provision of services; e) The transfer is reasonably necessary for reasons of public interest; or f) The transfer is reasonably necessary to respond to an emergency that threatens the life, health, or safety of the data principal or a third party.	

Issue	Current Clause	Recommendation	Rationale
		~~2. — Any personal data other than those categorised as sensitive personal data may be transferred outside the territory of Pakistan under the conditions to be devised by the Commission.~~ ~~3. — The Commission shall also devise a mechanism for keeping some components of the sensitive personal data in Pakistan to which this Act applies, on the grounds of public interest of national security.~~	
Extraterritorial application	2. APPLICATION.— 1. This Act shall apply – a. Where a person collects, processes, discloses, or shares personal data of a data principal whether online or offline within the territory of Pakistan; b. Where the State, any Pakistani company, any citizen of Pakistan or any person or body of persons incorporated or created under Pakistani law processes the personal data of a data principal; c. Where any data fiduciaries or data processors not having a physical presence within the territory of Pakistan carries out the processing of personal data if such processing is – i. concerning any commercial or non-commercial activity offering goods or services to data principals; or which involves profiling data principals within the territory of Pakistan. 2. shall not apply to the processing of anonymised data.	2. APPLICATION.— This Act shall apply to – a. ~~Where a person collects, processes, discloses, or shares personal data of a data principal whether online or offline within the territory of Pakistan;~~ b. ~~Where~~ the State, any Pakistani company, any citizen of Pakistan or any person or body of persons incorporated or created under Pakistani law ~~who~~ processes the personal data of a data principal; c. ~~Where~~ any data fiduciaries or data processors not ~~having a physical presence~~ established within the territory of Pakistan ~~who~~ carries out the processing of personal data ~~of data principals located in Pakistan, where if~~ such processing is related to – i. ~~concerning any commercial or non-commercial activity~~ the offering of goods or services to data principals ~~in Pakistan; or~~ i. ~~which involves~~ profiling data principals within the territory of Pakistan. ~~shall not apply to the processing of anonymised data.~~ his Act shall not apply to the processing of anonymised data or pseudonymised data.	• We recommend aligning the extraterritorial application of the Bill with international benchmarks, in particular that under Art 3 of the EU’s General Data Protection Regulation (“GDPR”). • Accordingly, we recommend that the Act applies to: (i) all processing by any data fiduciary or processor established in Pakistan; (ii) any data fiduciary or processor <i>not</i> established in Pakistan who targets and processes the personal data of data principals in Pakistan. A clearly defined jurisdictional scope is important for both organisations and data principals who seek to understand and manage their privacy obligations and rights. • Section 2(1)(a) is deleted to remove the overlap of extra-territoriality with section 2(1)(c). • A definition of “pseudonymised data” is introduced and section 2(2) clarifies that the Act does not apply to anonymised data or pseudonymised data – this is aligned with the alternative MOITT Bill.

Issue	Current Clause	Recommendation	Rationale
		<i>To include a new definition of “pseudonymised data” in section 3:</i> “Pseudonymised data” means the personal data that has been processed in such a manner that the personal data can no longer be attributed to a specific data principal without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.	
Sensitive personal data	3. DEFINITIONS gg) “Sensitive personal data” means any personal data revealing, related to, or constituting, as may be applicable— i. Passwords; i. financial data; i. health data; v. official identifier; v. sex life; i. sexual orientation; i. biometric data; i. genetic data; x. transgender status; x. intersex status; i. caste or tribe; 17. PROCESSING SENSITIVE PERSONAL DATA BASED ON EXPLICIT CONSENT 1. A data fiduciary shall process sensitive personal data if such processing is strictly required for:	3. DEFINITIONS gg) “Sensitive personal data” means any personal data revealing, related to, or constituting, as may be applicable— ~~i. Passwords;~~ ~~i. financial data;~~ i. health data; ~~v. official identifier;~~ v. sex life; i. sexual orientation; i. biometric data; i. genetic data; x. transgender status; x. intersex status; i. caste or tribe; 17. PROCESSING SENSITIVE PERSONAL DATA BASED ON EXPLICIT CONSENT (1) A data fiduciary shall not process any sensitive personal data except where the data principal has given explicit consent to the processing of those personal data for one or more specified purposes. A data fiduciary shall	• We recommend that passwords and financial data are removed from the definition of sensitive personal data. • The purpose of ‘sensitive data’ in global privacy laws is typically to add extra protection for data that reveals aspects of a person that are difficult to change and could expose that individual to discrimination or harm. Usual examples include aspects like race, sexual orientation and health data. • Passwords may not in some cases even be able to identify an individual. In addition, not all types of financial data are always higher risk to individual privacy and so a blanket inclusion of all financial data (which may include, for example, a bank account number which is generally necessary to make payments to an account) would not be proportionate to the increased protection provided to such sensitive personal data. • We recommend amending section 17 to make it clear that processing of sensitive data may be carried out with explicit consent.

Issue	Current Clause	Recommendation	Rationale
	a. any official function of the Government, Parliament or any provincial legislature; b. any legit function of the State that is for the ultimate benefit of the data principal. 18. PROCESSING SENSITIVE PERSONAL DATA IN CONNECTION WITH LAW OR ANY COURT ORDER.— 1. A data fiduciary shall process sensitive personal data if such processing is: a. for, or in connection with any legal proceedings, or any law enacted by the parliament or any provincial legislature; or b. to establish, exercise or defend legal rights; or c. to comply with the orders of any court or Tribunal in Pakistan. 19. PROCESSING SPECIFIC CATEGORIES OF SENSITIVE PERSONAL DATA.— 1. A data fiduciary shall process sensitive personal data such as passwords, financial data, health data, official identifiers, genetic data, and biometric data if such processing is strictly for the following purposes – a. for medical reasons and is undertaken by a healthcare professional to respond to any medical emergency involving a threat to the life or health of a data principal; b. to provide urgent medical care or health services to any individual during a pandemic, epidemic, or any other threat to public health; or c. to ensure the safety of, or aid or services to, any individual during any disaster or any breakdown of public order.	~~process sensitive personal data if such processing is strictly required for:~~ ~~a. any official function of the Government, Parliament or any provincial legislature;~~ ~~b. any legit function of the State that is for the ultimate benefit of the data principal.~~ 18. PROCESSING SENSITIVE PERSONAL DATA IN CONNECTION WITH LAW OR ANY COURT ORDER.— (1) ~~Notwithstanding section 17, a data fiduciary shall~~ may process sensitive personal data ~~without explicit consent~~ if such processing is: a. for any official function of the Government, Parliament or any provincial legislature; b. any legitimate function of the State that is for the ultimate benefit of the data principal. c. for, or in connection with any legal proceedings, or any law enacted by the parliament or any provincial legislature; or d. to establish, exercise or defend legal rights; or e. to comply with the orders of any court or Tribunal in Pakistan. 19. PROCESSING ~~SPECIFIC CATEGORIES OF~~ SENSITIVE PERSONAL DATA ~~WITHOUT CONSENT~~.— (1) ~~Notwithstanding section 17, a data fiduciary shall~~ may process sensitive personal data ~~such as passwords, financial data, health data, official identifiers, genetic data, and biometric data~~ if such processing is strictly for the following purposes – f. for medical reasons and is undertaken by a healthcare professional to respond to any medical emergency involving a threat	- We recommend deleting the references to “health data, official identifiers, genetic data, and biometric data” in section 19 since they are unnecessary given the definition of “sensitive personal data”. - The Commission’s power in section 20(1) to designate further categories of data as sensitive personal data is deleted for greater certainty for compliance. - The Commission’s power under section 20(2) to prescribe further protections or restrictions on the processing of sensitive personal data where the repeated, continuous or systematic collection of such data for profiling takes place is also deleted as the lack of general principles relating to processing of sensitive personal data at this primary legislation level creates confusion and uncertainty for those organisations seeking to comply.

Issue	Current Clause	Recommendation	Rationale
	20. FURTHER CATEGORIES OF SENSITIVE PERSONAL DATA.— - The Commission may notify further categories of personal data as sensitive personal data as deemed fit. - The Commission may also notify further categories of personal data as sensitive personal data requiring additional protections or restrictions where repeated, continuous, or systematic collection for profiling takes place.	to the life or health of a data principal or another individual; - to provide urgent medical care or health services to any individual during a pandemic, epidemic, or any other threat to public health; or - to ensure the safety of, or aid or services to, any individual during any disaster or any breakdown of public order; or the processing relates to personal data which are manifestly made public by the data principal. ~~20. FURTHER CATEGORIES OF SENSITIVE PERSONAL DATA.—~~ ~~(1) — The Commission may notify further categories of personal data as sensitive personal data as deemed fit.~~ ~~(2) — The Commission may also notify further categories of personal data as sensitive personal data requiring additional protections or restrictions where repeated, continuous, or systematic collection for profiling takes place.~~	
Processing data related to children	3. DEFINITIONS c) “Child” means a person who has not attained the age of eighteen years; 15. PROCESSING DATA RELATED TO CHILDREN.— - Every data fiduciary shall process a child’s personal data in such a manner that protects the rights and interests of the child. - The data fiduciary shall, before processing any personal data relating to a child, verify his age and seek the consent of his parent or	3. DEFINITIONS c) “Child” means a person who has not attained the age of thirteen eighteen years; 15. PROCESSING DATA RELATED TO CHILDREN.— 15. PROCESSING DATA RELATED TO CHILDREN.— Every data fiduciary shall process a child’s personal data in such a manner that protects the rights and interests of the child. The data fiduciary shall, before processing any personal data relating to a child, take reasonable	Age of a child: The age of a child for the purposes of a privacy law should be 13 years of age. This aligns with the US Children’s Online Privacy Protection Act (“COPPA”), GDPR and guidelines under Singapore’s Personal Data Protection Act (“PDPA”). Otherwise, there is a risk that teens will be locked out of the digital economy. The Bill as currently drafted risks barring teens from accessing educational resources online. Age verification: We recommend fiduciaries should be required to take reasonable steps to verify age but that the law should not

Issue	Current Clause	Recommendation	Rationale
	relevant person or authorized person having parental responsibility over the child to decide on his behalf. 3. The manner for age verification and parental consent under sub-section (2) shall be prescribed by rules to process children's data, taking into consideration: a. the volume of personal data processed; b. the proportion of such personal data likely to be that of the child; c. possibility of harm to the child arising out of the processing of personal data; and d. such other factors as may be prescribed. 4. A data fiduciary shall not process any personal data of a child that is likely to cause him harm, as prescribed under this Act. 5. A data fiduciary shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children. 6. The provisions of sub-section (1) and (3) shall not apply to the processing of the personal data of a child for such purposes, as may be prescribed in this Act.	steps to verify his age and seek the consent of his parent or relevant person or authorized person having parental responsibility over the child to decide on his behalf. ~~The manner for age verification and parental consent under sub-section (2) shall be prescribed by rules to process children's data, taking take into consideration:~~ ~~e volume of personal data processed;~~ ~~e proportion of such personal data likely to be that of the child;~~ ~~ssibility of harm to the child arising out of the processing of personal data; and~~ ~~ch other factors as may be prescribed.~~ A data fiduciary shall take reasonable steps not to process any personal data of a child that is likely to cause him harm, as prescribed under this Act. ~~A data fiduciary shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children.~~ The provisions of sub-section (1) ~~and (3)~~ shall not apply to the processing of the personal data of a child for such purposes, as may be prescribed in this Act.	prescribe specific age verification mechanisms. No single method of age verification mechanism can achieve 100% accuracy and prescribed methods may unduly increase costs and negatively impact a consumer's experience without actually protecting the child. The prohibition on all types of tracking, behavioural monitoring and targeted advertising in section 15(5) is deleted. Behavioural monitoring and personalisation is often a key part of online services which is used for beneficial purposes. For example, targeting is used to ensure that only age-appropriate advertisements and content is shown to children. The requirement as drafted would cause organisations to either have to implement severely reduced versions of their services to children, or else block them from a country altogether which would be detrimental to the broader public.
Consent for data processing	6. CONSENT FOR DATA PROCESSING.— Notwithstanding sub-section (1), a data fiduciary may process data of a data principal: a. if the processing is necessary for the performance of a contract to which the data principal is a party; b. for the taking steps at the request of the data principal to enter into a contract; c. for compliance with any legal obligations to which the data fiduciary is the subject, other than an obligation imposed by a contract;	6. CONSENT FOR DATA PROCESSING.— Notwithstanding sub-section (1), a data fiduciary may process data of a data principal: a. if the processing is necessary for the performance of a contract to which the data principal is a party; b. for the taking steps at the request of the data principal to enter into a contract; c. for compliance with any legal obligations to which the data fiduciary is the subject, other than an obligation imposed by a contract;	<u>Ideal redlines</u> The original section 6(6) does not contain an exception which permits personal data to be processed without consent where it is in the legitimate interests of the data fiduciary. This has been added as a new section 6(6)(i). An exception to permit the processing of personal data without consent where it is in the "legitimate interests" of the data fiduciary aligns with the approach adopted under

Issue	Current Clause	Recommendation	Rationale
	d. for protecting the vital interests of the data principal; e. for treatment, public health, medical or research purposes or to respond to any medical emergency involving a threat to the life or the health of a data principal or any other individual; f. for compliance with any court order of competent jurisdiction; g. for the exercise of any functions conferred under any law; h. for the exercise of any function of the Government authorized by law for the provision of any service or benefit, or the issuance of any certification, license or permit;	d. for protecting the vital interests of the data principal; e. for treatment, public health, medical or research purposes or to respond to any medical emergency involving a threat to the life or the health of a data principal or any other individual; f. for compliance with any court order of competent jurisdiction; g. for the exercise of any functions conferred under any law; h. for the exercise of any function of the Government authorized by law for the provision of any service or benefit, or the issuance of any certification, license or permit; or i. for legitimate interests pursued by the data fiduciary.	international benchmark legislation such as the GDPR.
Notice	8. NOTICE.— 1. A data fiduciary shall by written notice inform a data principal or where this is not practical, it shall be provided by a data processor of the data fiduciary that exercises control over the same personal data— a. with an itemised notice containing a description and categories of personal data sought to be collected; b. provide the legal basis for the processing of personal data and the duration for which data is likely to be processed and retained thereafter for further processing; c. inform the data principal about their rights as mentioned in Chapter V and provide information on contacting the data fiduciary in case of inquiries or complaints concerning personal data;	8. NOTICE.— A data fiduciary shall by written notice inform a data principal or where this is not practical, it shall be provided by a data processor of the data fiduciary that exercises control over the same personal data— i. ~~with an itemised notice containing~~ a description ~~and of the~~ categories of personal data sought to be collected; ii. provide the legal basis for the processing of personal data and the duration for which data is likely to be processed and retained thereafter for further processing; iii. inform the data principal about their rights as mentioned in Chapter V and provide information on contacting the data fiduciary in case of inquiries or complaints concerning personal data; iv. provide the list of the categories of third parties to whom the data fiduciary will disclose or may disclose the personal data;	- The requirement in section 8(1)(a) to provide an “itemised notice containing a description and categories of personal data sought to be collected” is too prescriptive and may result in notice fatigue for data principals if the expectation is for an extensive amount of detail to be provided for the “itemised notice”. - In order to avoid excessive notice fatigue and to reduce the costs of constantly updating specific lists of third-party recipients, data fiduciaries and data processors should be permitted in section 8(1)(d) to disclose the categories of third-party recipients as this provides sufficient transparency without overloading the data principal with too much information that does not necessarily increase privacy protections. - The Commission’s power to prescribe further types of information that needs to be included in the notice under Section 8(1)(i) of the Bill

Issue	Current Clause	Recommendation	Rationale
	d. provide the list of third parties to whom the data fiduciary will disclose or may disclose the personal data; e. the choices and means, the data fiduciary offer the data principal for restricting the processing of personal data, including personal data relating to other persons who may be identified from that personal data; f. information regarding any cross-border transfer of personal data that the data fiduciary intends to carry out, if applicable; g. whether it is obligatory or voluntary for the data principal to supply the personal data; and h. where it is obligatory for the data principal to provide personal data, but in case of failure to comply with the request shall face the consequences; i. any other information as may be specified by the Commission.	v. the choices and means, the data fiduciary offer the data principal for restricting the processing of personal data, including personal data relating to other persons who may be identified from that personal data; i. information regarding any cross-border transfer of personal data that the data fiduciary intends to carry out, if applicable; i. whether it is obligatory or voluntary for the data principal to supply the personal data; and i. where it is obligatory for the data principal to provide personal data, but in case of failure to comply with the request shall face the consequences; ~~k. any other information as may be specified by the Commission.~~	should be deleted. There is limited merit in giving the Commission the power to prescribe additional information that needs to be included in privacy notices, as the content of the privacy notice is not expected to evolve over time or with changes in technology.
Security requirements	10. SECURITY REQUIREMENTS.— 1. Given the national interest, the Commission shall prescribe the best international practices for protecting personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration, or destruction. 2. A data fiduciary or data processor shall process personal data by employing appropriate technical and organisational security standards to protect the personal data from the incidents mentioned under sub-section (1): a. to the place or location where the personal data is stored;	10. SECURITY REQUIREMENTS.— (1) Given the national interest, the Commission shall ~~prescribe~~ issue non-binding guidelines on the best international practices for protecting personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration, or destruction. (2) A data fiduciary or data processor shall process personal data by employing appropriate technical and organisational security standards to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration, or destruction ~~the incidents mentioned under sub-section (1):~~	• We agree that guidance from the Commission on international best practices for protection data will be helpful for industry. However, we recommend that guidance is in the form of non-binding guidelines, rather than prescribed regulations. • Prescriptive security standards are unlikely to be able to cover all different types of data fiduciaries and will not be technology neutral. They are therefore likely to be out of date quickly. They may inadvertently become arbitrary, increase compliance costs for organisations, and may not always result in tangible benefits for the data principal. There should be flexibility for organisations to decide what security controls are suited for the types of personal data, processing

Issue	Current Clause	Recommendation	Rationale
	b. to any security measures incorporated into any equipment in which the personal data is stored; c. to the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and d. to the measures taken for ensuring the secure transfer of personal data. 3. On behalf of the data fiduciary, if a data processor carries out the processing of personal data to protect it from the incidents mentioned in sub-section (1), the data fiduciary must ensure the data processor's compliance with technical and organisational security standards, as prescribed by the Commission. 4. The data processor is independently liable to ensure compliance with security standards prescribed under sub-section (1).	a. to the place or location where the personal data is stored; b. to any security measures incorporated into any equipment in which the personal data is stored; c. to the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and d. to the measures taken for ensuring the secure transfer of personal data. (3) On behalf of the data fiduciary, if a data processor carries out the processing of personal data ~~the data fiduciary shall also be responsible for the data processor's compliance with sub-section (1). to protect it from the incidents mentioned in sub-section (1), the data fiduciary must ensure the data processor's compliance with technical and organisational security standards, as prescribed by the Commission.~~ (4) The data processor is independently liable to ensure compliance with ~~security standards prescribed under~~ sub-section (12).	activities, and based on best industry practice. Section 10.2 of the Bill already requires that the security measures implemented be appropriate to protect personal data from security incidents. This requirement is sufficient and is consistent with global privacy norms. The other edits to sections 10(3) and 10(4) are consequential edits following the deletion of 10(1).
Right to erasure	25. RIGHT TO ERASURE.— The data principal shall have the right to request the data fiduciary the erasure of personal data concerning him without undue delay, therefore, the data principal shall have the obligation to erase personal data within a period of 14 days where one or more of the following condition applies: a. the personal data are no longer necessary concerning the purposes for which they were collected or otherwise processed; b. the data principal withdraws consent on which the processing is based under sub-section	25. RIGHT TO ERASURE.— The data principal shall have the right to request the data fiduciary the erasure of personal data concerning him without undue delay, ~~therefore, the data principal shall have the obligation to erase personal data within a period of 14 days~~ where one or more of the following condition applies: a. the personal data are no longer necessary concerning the purposes for which they were collected or otherwise processed; b. the data principal withdraws consent on which the processing is based under sub-section (1) of section 26 and where there is no other legal ground for the processing; or	- We agree that data fiduciaries should be required to process a deletion request without undue delay. This is consistent with the GDPR. - However, we recommend that the reference to deletion being required within 14 days is deleted. - Short, prescriptive timelines pose a significant administrative burden for businesses, in particular small enterprises, and fail to recognise that different cases require different response times, depending on the complexity of the request. It will not always be technically possible to execute deletion

Issue	Current Clause	Recommendation	Rationale
	(1) of section 26 and where there is no other legal ground for the processing; or c. the data principal objects to the processing under sub-section (1) of section 26; d. the data have been unlawfully processed; or e. the data must be erased in compliance with a legal obligation. Without prejudicing the rights of the person protected under the Act, subsections (1) and (2) shall not apply to the extent that any processing is necessary: a. for exercising the right of freedom of expression and information; b. for compliance with a legal obligation or the performance of a task carried out in the public interest; c. for reasons of public interest in the area of public health; d. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes as the right referred to in subsection (1) is likely to render impossible or seriously impair the achievement of the objectives of that processing; or e. for the establishment, exercise or defence of legal claims.	c. the data principal objects to the processing under sub-section (1) of section 26; d. the data have been unlawfully processed; or e. the data must be erased in compliance with a legal obligation. ~~Without prejudicing the rights of the person protected under the Act,~~ Subsections (1) and (2) shall not apply to the extent that any processing is necessary: a. for exercising the right of freedom of expression and information; b. for compliance with a legal obligation or the performance of a task carried out in the public interest; c. for reasons of public interest in the area of public health; d. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes as the right referred to in subsection (1) is likely to render impossible or seriously impair the achievement of the objectives of that processing; or e. for the establishment, exercise or defence of legal claims.	within 14 days, even where a fiduciary is acting without undue delay. A time standard of 14 days would be inconsistent with global norms. The qualification in section 25(3) that the exceptions to the right of erasure are subject to the exceptions not “prejudicing the rights of the persons protected under the Act” is vague. It also implies that data fiduciaries must now conduct a balancing test before they can rely on any of the listed exemptions. it is unclear what conduct would be considered to prejudice the rights of a person and so we recommend deleting this.
Notification of data processing to Commission	13. RECORD TO BE KEPT BY THE DATA FIDUCIARY.— A data fiduciary shall keep and maintain a record of each application, notice, request, or any other information concerning the processed personal data. The manner and form in which the record is to be maintained would be determined by the Commission.	13. RECORD TO BE KEPT BY THE DATA FIDUCIARY.— A data fiduciary shall keep and maintain a record of each application, notice, request, or any other information concerning the processed personal data. The manner and form in which the record is to be maintained would be determined by the Commission.	The ongoing requirement in section 13(2) to regularly report to the Commission the types of data collected and the processing activities undertaken is burdensome to both the Commission and each organisation and should be deleted.

Issue	Current Clause	Recommendation	Rationale
	The data fiduciary shall apprise the Commission regularly about the type of data they are collecting, and the processing undertaken on the collective data. This shall not apply in situations where the data collection is occasional unless the processing results in the infringement of the fundamental rights and freedoms of the data principal, as enshrined in the Constitution of Pakistan.	~~The data fiduciary shall apprise the Commission regularly about the type of data they are collecting, and the processing undertaken on the collective data. This shall not apply in situations where the data collection is occasional unless the processing results in the infringement of the fundamental rights and freedoms of the data principal, as enshrined in the Constitution of Pakistan.~~	The section 13(2) requirement to regularly report the type of data being processed is out-of-step with international benchmarks and is extremely burdensome to the Commission given that practically all organisations process personal data in some form or another.
Registration framework	40. POWERS OF THE COMMISSION Without prejudice to the generality of the foregoing power, the Commission shall- (...) (e) Formulate a Registration Framework for data fiduciaries and data processors under the Act;	40. POWERS OF THE COMMISSION Without prejudice to the generality of the foregoing power, the Commission shall- (...) ~~(e) Formulate a Registration Framework for data fiduciaries and data processors under the Act;~~	- The Commission's power in section 40(2)(e) to implement a registration and licensing framework for data fiduciaries and data processors should be deleted. A registration and licensing framework would be out of step with most regional laws and international benchmarks including the OECD Privacy Guidelines, the GDPR, Singapore's PDPA and Australia's Privacy Act. This would be an unnecessary administrative burden for the government, increase compliance costs for organisations (particularly if registration fees and annual fees are imposed), and may not lead to a meaningful increase in compliance by organisations or enhance privacy protections for data principals. - Given the nature of the internet and accessibility of almost any website by users in Pakistan, this also may result in international companies and services pre-emptively geo-blocking their services from the Pakistan market so as not to be subject to the registration requirement, which would undoubtedly result in less choice and benefits for consumers. Registration does not necessarily lead to meaningful compliance by

Issue	Current Clause	Recommendation	Rationale
			organisations because even if offshore organisations do register with local regulators, the practical challenges of enforcement against offshore entities still remains, together with the ongoing risk of organisations geo-blocking their services from Pakistan as highlighted above.
Regulations for big / large data fiduciaries and processors	40. POWERS OF THE COMMISSION Without prejudice to the generality of the foregoing power, the Commission shall- (...) (d) Identify big/large data fiduciary/processors, along with other categories, and define special measures for compliance by the provisions of the Act;	40. POWERS OF THE COMMISSION Without prejudice to the generality of the foregoing power, the Commission shall- (...) ~~(d) Identify big/large data fiduciary/processors, along with other categories, and define special measures for compliance by the provisions of the Act;~~	- The Commission's power in section 40(2)(d) to formulate specific regulations for "big/large data fiduciary/processors, along with other categories" should be deleted. It is unclear what definition will be applied to "big/large data fiduciary/processors, along with other categories" and what additional restrictions will be imposed on such organisations, therefore generating significant uncertainty around compliance obligations for businesses of all sizes. - Privacy laws should in general adopt a consistent approach to privacy and imposing additional restrictions based on the size of the data fiduciary or processor would be arbitrary and may not result in greater protection for data subjects. The nature of the personal data and processing is far more relevant to protecting the personal data and privacy of data subjects than the scale.
Fines	CHAPTER VIII: COMPLAINT AND OFFENCES 47. UNLAWFUL PROCESSING OF PERSONAL DATA.— Where a data fiduciary or a data processor process, disseminates or discloses any personal data in violation of any of the provisions of this Act shall be punished with fine up to fifteen	CHAPTER VIII: COMPLAINT AND OFFENCES 47. UNLAWFUL PROCESSING OF PERSONAL DATA.— (1) Where a data fiduciary or a data processor process, disseminates or discloses any personal data in violation of any of the provisions of this Act shall be punished with	- The quantum of fines for non-compliance with the provisions of the Act is high (e.g. USD 5.5 million for a first time offence under section 47(1)). We recommend that the maximum fines proposed be consistent with those proposed under the MOITT Bill. - We further recommend that any fine should be limited in scale by reference to local turnover in Pakistan, not global turnover.

Issue	Current Clause	Recommendation	Rationale
	hundred million rupees and in case of subsequent unlawful processing of personal data, the fine may be raised to twenty-five hundred million rupees. In case, where the offence is committed under sub-section (1) and relates to sensitive data the offender may be punished with a fine of up to five thousand million rupees or up to 2% of its global turnover of the preceding fiscal year, whichever is a higher penalty, shall be assessed by the Commission. Explanation: For the purpose of this section, “total global turnover” means the gross amount of revenue recognised in the profit and loss account of any other equivalent statement of a data fiduciary where such revenue is generated within Pakistan and outside Pakistan. 48. FAILURE TO ADOPT APPROPRIATE DATA SECURITY MEASURES.— Where a data fiduciary or a data processor fails to take adequate security measures to prevent a data breach, as per the provisions laid down in this Act shall be punished with a fine of up to twenty-five hundred million rupees. ISSUE ENFORCEMENT ORDERS AND IMPOSE PENALTIES.— Where a data fiduciary or a data processor fails to comply with the orders of the Commission or the court when required to do so, shall be punished with a fine of up to five hundred million rupees. Where anyone fails to: - a. respond to the notice referred to in subsection (1);	fine up to fifteen ~~hundred~~ million rupees and in case of subsequent unlawful processing of personal data, the fine may be raised to twenty-five ~~hundred~~ million rupees. (2) ~~In case, where the offence is committed under sub-section (1) and relates to sensitive data the offender~~ Anyone who processes or cause to be processed, disseminates or discloses sensitive personal data in violation of any of the provisions of this Act may be punished with a fine of up to ~~five thousand~~ twenty five million rupees or up to 2% of its ~~global~~ local turnover of the preceding fiscal year, whichever is a higher penalty, ~~shall be assessed by the Commission.~~ Explanation: For the purpose of this section, “~~total~~ ~~global~~ local turnover” means the gross amount of revenue recognised in the profit and loss account of any other equivalent statement of a data fiduciary where such revenue is generated within Pakistan ~~and outside Pakistan.~~ 48. FAILURE TO ADOPT APPROPRIATE DATA SECURITY MEASURES.— (1) Where a data fiduciary or a data processor fails to take adequate security measures to prevent a data breach, as per the provisions laid down in this Act shall be punished with a fine of up to twenty-five ~~hundred~~ million rupees. 49. ISSUE ENFORCEMENT ORDERS AND IMPOSE PENALTIES.— (1) Where a data fiduciary or a data processor fails to comply with the orders of the Commission or the court when required to	Revenue generated outside Pakistan is not and cannot be relevant to breaches of the Pakistan law and therefore should not be a factor in determining the quantum of fines. While enforcement frameworks are a necessary part of privacy laws, best practice in developing such enforcement frameworks strongly suggests that a carefully calibrated enforcement strategy coupled with greater awareness from education and outreach programmes are key to promoting compliance. Specifically, leading international frameworks, such as the GDPR and the Singapore PDPA, focus on the key principles of fairness, proportionality, accountability, constructive engagement, and mutual trust. Successful enforcement strategies are those that focus on fostering trust between the regulator and the regulated, promoting accountability mechanisms such as codes of practice, and cautiously using punitive sanctions only as a last resort.

Issue	Current Clause	Recommendation	Rationale
	b. satisfy the Commission about the alleged contravention; or c. provide redressal in writing and providing satisfactory reasons for the contravention within the time allowed by the Commission, shall be- i. Levied with a fine which may extend to five hundred million rupees; i. Faced with a suspension or termination of the registration and shall be imposed with stringent conditions.	do so, shall be punished with a fine of up to five ~~hundred~~ million rupees. (...) (4) Where anyone fails to: - a. respond to the notice referred to in subsection (1); b. satisfy the Commission about the alleged contravention; or c. provide redressal in writing and providing satisfactory reasons for the contravention within the time allowed by the Commission, shall be- i. Levied with a fine which may extend to five ~~hundred~~ million rupees; ~~i. Faced with a suspension or termination of the registration and shall be imposed with stringent conditions.~~	
Calculation of Fines	No current clause.	49A. GENERAL CONDITIONS FOR IMPOSING ADMINISTRATIVE FINES (1) When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following: (a) the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data principals affected and the level of damage suffered by them; (b) the intentional or negligent character of the infringement; (c) any action taken by the data fiduciary or processor to mitigate the damage suffered by data principals; (d) the degree of responsibility of the data fiduciary or processor taking into account	• We recommend that provisions are adopted into the Bill to guide the imposition of fines which are consistent with global privacy norms. We have suggested some provisions which are drawn from GDPR Article 83. • Not all infringements will be equal in gravity and the fines listed in sections 47, 48 and 49 are maximum fines. Therefore, it is important that the Commission has regard to specified factors in determining what quantum of fine to impose. • Similarly, given the interconnectedness of modern digital processing, it is likely that where there is a course of conduct resulting in a breach of the Act there may be other technical breaches of the Act. In these circumstances, there should be one fine imposed in relation to those processing activities which is set by reference to the

Issue	Current Clause	Recommendation	Rationale
		technical and organisational measures implemented by them; (e) any relevant previous infringements by the data fiduciary or processor; (f) the degree of cooperation with the Commission, in order to remedy the infringement and mitigate the possible adverse effects of the infringement; (g) the categories of personal data affected by the infringement; (h) the manner in which the infringement became known to the Commission, in particular whether, and if so to what extent, the data fiduciary or processor notified the infringement; (i) where measures referred to in Section 40(j) have previously been ordered against the data fiduciary or processor concerned with regard to the same subject-matter, compliance with those measures; and (j) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement. (2) If a data fiduciary or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Act, the total amount of the fine shall not exceed the amount specified for the gravest infringement.	penalty amount which may be imposed for the gravest contravention.
Definition of “fiduciary”	3. DEFINITIONS l) “Fiduciary” means an agent, who has rights and powers normally belonging to another person or to a principal, that must be exercised with a high standard of loyalty and care, for the benefit of the beneficiary or a principal;	3. DEFINITIONS ~~l) “Fiduciary” means an agent, who has rights and powers normally belonging to another person or to a principal, that must be exercised with a high standard of loyalty and care, for the benefit of the beneficiary or a principal;~~	The separate definition of “fiduciary” in section 3(l) should be deleted. The separate definition for “fiduciary” (in addition to the definition of “data fiduciary”) is out of step with the controller/processor distinction used in other international benchmark laws. The

Issue	Current Clause	Recommendation	Rationale
			concept of a “fiduciary” exercising rights and powers belonging to a principal is also not a commonly found concept in international benchmark laws, and so this could create confusion for international organisations operating in Pakistan. This could potentially lead to the unintended effect of non-Pakistan based companies geo-blocking some or all of their services and resources so that they will not be accessible to Pakistani users, as a precautionary measure to avoid inadvertently taking on additional measures as a “fiduciary” under the law. In any case, there is an overlap between the definitions of “data fiduciary” and “fiduciary”, and this creates further confusion as to what constitutes a data fiduciary regulated under the Act. The definition of “fiduciary” in the Act considers the fiduciary to be an agent of a principal, but this is not necessarily a reflection of every single relationship between a data fiduciary and a data principal (as such data fiduciary-data principal relationships could include service provider-customer and employer-employee relationships). There is a risk that definitional ambiguity could result in certain types of “controller” organisations falling outside of the definition of a data fiduciary and accordingly not being subject to the provisions of the Bill.
Definition of “data breach”	3. DEFINITIONS (h) "Data breach" means the unauthorised access, collection, use, disclosure, copying, modification, or disposal of personal data or the loss of any storage medium or device on which personal data is stored in circumstances where unauthorised access, collection, use, disclosure, copying,	3. DEFINITIONS ~~(h) "Data breach" means the unauthorised access, collection, use, disclosure, copying, modification, or disposal of personal data or the loss of any storage medium or device on which personal data is stored in circumstances where unauthorised access, collection, use, disclosure, copying,~~	The definition is not needed as there is a separate definition of “personal data breach” at section 3(x).

Issue	Current Clause	Recommendation	Rationale
	modification, or disposal of the personal data is likely to occur;	~~modification, or disposal of the personal data is likely to occur;~~	
Data processing exemptions	29. RIGHT TO AVOID REPEATED COLLECTION.— (...) 32. EXEMPTION.— (...) 33. REPEATED COLLECTION OF PERSONAL DATA.— (...)	<i>Move these sections to a separate Chapter for “Exemptions.”</i>	- As it is currently drafted, the exemptions from the notice and consent obligations for repeated data collection are listed under both the “Data Principal Rights” (see section 29) and “Transfer of Personal Data Outside Pakistan” (see section 33) chapters. - The “exemptions” under section 33 appear to be general exemptions to the notice, consent and disclosure obligations but they are listed under the “Transfers of Personal Data Outside Pakistan” chapter. This is taxonomically confusing and there is a risk that with the current drafting, the exemptions being read differently/more narrowly than what was originally intended by the drafter.